Revealing the Cyber Security Non-Compliance "Attribution Gulf"

Jacques Ophoff
Abertay University, Scotland
j.ophoff@abertay.ac.uk

Karen Renaud
Abertay University, Scotland
Rhodes University, South Africa
k.renaud@abertay.ac.uk

Abstract

Non-compliance is a well-known issue in the field of cyber security. Non-compliance usually manifests in an individual's sins of omission or commission, and it is easy to conclude that the problem is attributable to their personal flawed decision making. However, the individual's decision not to comply is likely also to be influenced by a range of environmental and contextual factors. Bordieu, for example, suggests that personal ***habitus*** *influences decisions. We identified a wide range of possible explanations for non-compliance from the research literature and classified these, finding that a number of the identified factors were indeed habitus related. We then used Q-methodology to determine which of these non-compliance explanations aligned with public attributions of non-compliance causatives. We discovered an "attribution gulf", with popular opinion attributing non-compliance primarily to individual failings or ignorance. The existence of this attribution gap means that those designing cyber security interventions are likely to neglect the influence of habitus on choices and decisions. We need to broaden our focus if non-compliance is to be reduced.*

1. Introduction

In the cybersecurity arena, people either *comply* with organisational information security policies [1, 2], *try but struggle* to comply [3] or actively *resist* [2, 4]. The latter, referred to as "non-compliance" in the cyber security context, is the focus of this paper because, as argued by Kirlappos *et al.*, [5] "*understanding non-compliant behaviors provides the basis for effective security*."

While the non-compliance phenomenon manifests as an individual resisting policy strictures, there are likely to be more complex reasons than individual intransigence, ignorance or poor security skills [6, 7]. Utesheva and Boell [8] argue that we cannot study the use of technology without giving due consideration to the social context within which it emerges. They argue for a more holistic approach. Sterne [9] cites Elias and Jephcott [10], who argue that our behaviors are socially informed, to their core, and that it is impossible to understand human behavior from a purely human cognition perspective. In this paper, we point to the influence of Bordieu's habitus in leading to non-compliant behaviors in the cyber domain. We also discovered that common wisdom in this area primarily attributes non-compliance to the individual user's cognition, which impoverishes organizations' ability to intervene successfully in this area. In this paper, we ask: "what is the nature of society's thinking about cybersecurity non-compliance?"

We set the scene in Section 2, proposing an extended habitus model to model the factors influencing human cybersecurity behaviors. Section 3 explains how we searched the literature review to identify non-compliance factors, which we allocated to different dimensions of the new "bigger picture" model. We then carried out a study to gauge opinions related to non-compliance causative attributions (Section 4). We discuss our findings and conclude in Section 5.

2. Scoping the Bigger Picture

In understanding non-compliance, we consider two dimensions. The first is that of the individual, their knowledge, biases and decision-making strategies (Section 2.1). We then introduce *habitus* (Section 2.2) and justify the extension of the traditional habitus model with cyber capital in Section 2.3.

2.1. Individual Issues

Non-compliance has been attributed to a range of individual factors including dishonesty [11], a lack of knowledge and awareness [5] and habit [12, 13, 14, 15], amongst others. While acknowledging the validity of these factors, we also argue that focusing on the individual, without giving due consideration to the dynamism of social aspects, might contribute

URI: https://hdl.handle.net/10125/71169
978-0-9981331-4-0

to the continuing intractability of the non-compliance issue in organisations [16]. We plan to use Bordieu's concept of Habitus, extended to meet the needs of the cyber era, to better understand all the factors that influence employees and trigger non-compliance with organizational cybersecurity policies.

2.2. Bordieu's Habitus

Human behavior is likely to be influenced by a concept suggested by Pierre Bordieu, called *habitus* [17]. Bourdieu suggests that habitus is about the power we have, with such power being a consequence of the different kinds of capital we have accumulated over our lifetimes.

Habitus is created as a consequence of the interplay between free will and structures over time, the product of ongoing processes of socialization [18]. These processes impart practices which are accepted and understood by society, but not necessarily encoded in written format. Habitus emerges from lived experiences and events and is also impacted by society's structures [19, p.170]. Habitus is created unconsciously, '*without any deliberate pursuit of coherence ... without any conscious concentration* [19, p.170]. Bordieu [17] calls it a kind of second nature.

Papacharissi and Easton [18] explain that the habitus concept is both ambiguous and flexible. However, rather than this being a weakness of the theory, they argue that these two characteristics give it the power to reflect how humans respond to structural features of their world, and that it does so by not separating structure from agency.

Bourdieu defines three forms of capital, which give us power in society: *social*, *cultural* and *economic*.

Social capital refers to the network of '*useful relationships that can secure material or symbolic profits*' [20, p.249] i.e. the number of people an individual can draw upon.

Cultural capital has three forms:

Embodied: This is the capital which is part of the person [20] i.e. within their bodies. It is accumulated during childhood, based on experiences and advantages accrued due to their relative position in society.

Objectified: This capital is related to the goods and artefacts the person owns which communicate with others [20]. The person might buy Apple products because they have more prestige than the alternatives, or display their well-populated bookshelf on Zoom calls to signal their highbrow choices.

Institutionalised: This capital refers to the person's academic qualifications that make it possible for an individual to convert between cultural and economic capital. Bourdieu refers to this capital as 'a certificate of cultural competence which confers on its holder a conventional, constant, legally guaranteed value with respect to culture' [20, p. 248]. So, someone with an Oxford degree would have higher institutionalised capital than a person with a degree from a post-1992 University in the UK.

Economic capital is related to the person's financial wealth, and is clearly connected to the careers we choose and the jobs we engage in, which all contribute to the accumulation of such wealth. Inherited wealth also falls into this category.

2.3. Extending Habitus

It could be argued that Bordieu's cultural capital is flexible enough to encompass modern day technology usage and cyber security rituals. This would align with Davies and Rizk's [21] narrative on how cultural capital has expanded and flexed to be useful within the educational domain. However, a number of researchers have argued for the existence of a technological capital to be included in the habitus model [22, 23].

The cyber field is indeed closely linked to the technological field. Yet, Bell [24] explains that the cyber world is different from the physical world. It not only makes use of technology, it also allows people to carve out their own identities, and to craft home pages that convey the image they want to convey. Moreover, the cyber field includes the concept of cyber criminals, something that the technological field does not grapple with. Technological capital thus does not appear to play a role in terms of non-compliance.

In the cybersecurity field, the distinctions between those *with* cybersecurity knowledge, and those *without*, is stark [25, 26]. Shia [27] highlights the digital cybersecurity divide in the global south, with the gap between the haves and have-nots being particularly visible and deleterious. Debb *et al.* [28] raises the age-related differences in online security behaviors. These are the kinds of factors that manifest in the differences in other kinds of habitus capital areas, which suggests that this kind of capital endows people with new modern kind of socially-imbued power. There is also a worldwide need for cybersecurity experts [29], once again suggesting that cyber capital is particularly valuable.

We thus conclude that it would be useful, for the purposes of our investigation, to consider cyber capital as a distinct kind of capital. Similar to [25, 22], we argue that separating this capital from others gives us the ability to examine non-compliance with information security policies related to the use of workplace technologies, and in identifying barriers to

compliance.

3. Methodology

To find out what the general public attributes non-compliance to, we first determine what factors the research literature refers to in this respect, and classify these in terms of the habitus capital types (Section 3.1). We then explain the Q-methodology mechanism, which we used to gauge subjectivity i.e. general attributions of non-compliance (Section 3.2). Finally, Section 3.3 explains how we recruited and remunerated our study participants.

3.1. Deriving Non-compliance Factors

There is an extensive literature into compliance in the information security domain, as reflected by a number of systematic literature reviews [30, 31, 32]. However, compliance and non-compliance are not always opposite sides of the same coin. Similar to acceptance and resistance factors [33], the factors that motivate compliance and those that lead to non-compliance can be different from each other [34]. Hence, in carrying out this review, we only searched for papers related to "information security" and "noncompliance or non-compliance." We then proceeded as follows:

Deriving: We worked through the papers to extract all non-compliance factors researchers cited. We then derived statements which we could use in our Q-sort procedure. We did this independently then met to refine and agree on final statements.

Consolidating: The authors worked through the list together to combine semantically similar factors and then translated these to statements which we could use in confirming public perceptions of the influence of these factors in leading to non-compliance (Table 1).

Categorizing: We then classified the factors as either within the individual or one of the other four habitus capital types in our extended model (Figure 1).

3.2. Assessing Subjectivity

To assess perceptions of the identified factors' influence, we used Q-methodology, a research method introduced by Stephenson [72] for the systematic study of subjectivity. Q-methodology is essentially an informal instantiation of Cultural Consensus Theory [73], which provides a framework for the measurement of beliefs *as cultural phenomena*. In other words, it allows us to assess beliefs shared by groups of individuals. As such, this theory helps us to assess what people consider to be the culturally appropriate answers

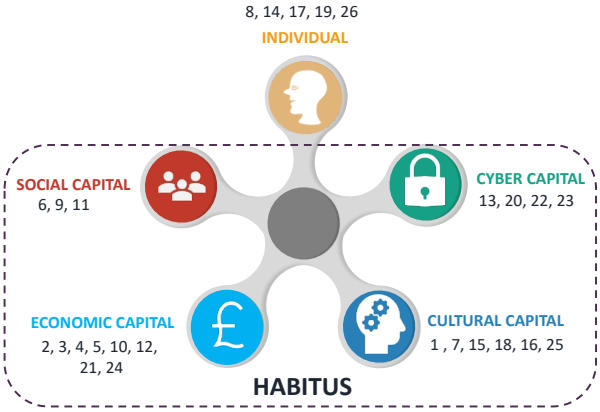

Figure 1. Mapping Factors to Habitus Capital Types & Individual Attributes (Numbers refer to Factors in Table 1)

to a series of related questions (the overriding theme, in our case, being cybersecurity non-compliance).

The findings are not meant to be representative of the general population, but rather to reveal the nature of subjectivity in this domain. Not '*how are people thinking on the topic?*', but rather: '*what is the nature of their thinking?*' This focus on segments of similar or dissimilar points of view renders the issue of large participant numbers '*relatively unimportant*' [74].

The method essentially seeks to reveal correlations between subjects across a sample of variables, referred to as the Q set and which is composed of Q statements. Factor analysis isolates the most influential "factors," which represent cultural ways of thinking. The method's strengths are that it applies sophisticated factor analysis, but also supports a qualitative analysis by eliciting responses which explain people's ranking of different statements. It is an exploratory technique which cannot prove hypotheses, but can provide a coherent view on '*potentially complex and socially contested*' issues [75]. Figure 2 details the steps participants engage in when doing a Q-sort.

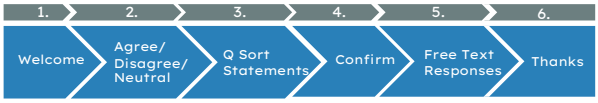

Figure 2. Q-Sorting Process

Participants sort the statements into a fixed quasi-normal distribution, ranging from -3 (disagree) to +3 (agree). Participants were given a chance to amend and confirm their rankings and then asked for open-ended comments for the most agreeable (ranked +3) and most disagreeable (ranked -3) statements. This

Table 1. Grouped Non-compliance Factors & Corresponding Q Statements

#	Factor	Source(s)	Q Statement	Capital
1	Neutralization strategies	[35, 36, 37]	People are satisfied that they can justify why they don't need to follow the rules.	Cultural
2	Perceived cost of non-compliance; Sanction likelihood; Sanction severity	[37, 35, 38, 39, 40, 41, 42]	There is little chance of being called out for not following the rules.	Economic
3	Perceived cost of compliance; Work Impediment; Perceived response cost	[37, 43, 5, 44, 45, 46, 13, 47]	It is just too troublesome to follow the rules.	Economic
4	Unrealistic task demands; Difficulty	[3, 37, 43, 5, 44, 45, 46, 13]	Cyber security gets in the way of doing their jobs.	Economic
5	Lack of sanctions; Incomplete monitoring	[38, 39]	There are few consequences for not following the rules.	Economic
6	Mistrust; Rules oriented environment; Strict IT governance; Rules-oriented ethical climate	[48, 49, 36, 11, 49, 11, 44, 50, 47, 51]	An unpleasant workplace environment.	Social
7	National culture	[52, 53, 48, 39]	Behavior is influenced by national culture.	Cultural
8	Anxiety; Fear; Information security stress; Negative affective flow	[43, 3, 54, 12, 55, 47]	People feel generally anxious, stressed, or fearful.	Individual
9	Behaviors of peers; Susceptibility to interpersonal influence; Social norms; Differential association	[43, 56, 57, 53, 58, 3, 57, 42, 42]	People are copying the behavior of their colleagues.	Social
10	Workload	[3, 54]	People are overloaded with work.	Economic
11	Being excluded from policy formulation	[3]	People are not allowed to feed into the creation of cyber security rules.	Social
12	Lack of resources	[3, 53, 48]	People lack physical resources (e.g. technology, money) to follow the rules.	Economic
13	Intuitive, overriding, and declarative cognitions; Lack of awareness	[59, 5, 47, 60, 60]	People lack knowledge and awareness of cyber security.	Cyber
14	Dishonesty	[11]	Dishonest people don't follow rules.	Individual
15	Shadow security (workarounds)	[5, 60, 61]	People find convenient alternatives to cyber security requirements.	Cultural
16	Rules are impossible to follow	[5, 3, 62, 60, 7]	It's too difficult, or impossible, to follow the rules.	Cultural
17	Values	[63, 64, 58]	The rules do not align with personal values.	Individual
18	Invasion of privacy	[54]	Following the rules violates personal privacy.	Cultural
19	Habit	[12, 13, 14, 15]	People prefer to do what they are used to doing.	Individual
20	Frustration	[55]	People feel frustrated with cyber security requirements.	Cyber
21	Perceived benefits of non-compliance	[65]	People believe there are benefits in NOT following the rules.	Economic
22	High over-confidence	[66]	People consider themselves too smart and therefore above the rules.	Cyber
23	Complacency; Loafing	[62, 67, 60]	People are not interested in cyber security.	Cyber
24	Rewards; Commitment	[13, 42]	People are not committed to cyber security, and only follow rules because of external rewards.	Economic
25	Poor business-IT alignment; Perceived policy argument	[68, 60]	People don't agree with the rationale behind the rules.	Cultural
26	Compliance Budget	[69, 70, 71]	People comply up to a point, and then they're done.	Individual

serves to get '*an impression of the range of opinion at issue*' [74].

3.3. Piloting, Recruitment & Remuneration

Five pilot tests were undertaken and timed, to get a sense for the time needed for the task. Based on feedback obtained from the pilot testers, unclear statements were subsequently refined and clarity improved.

Forty participants were recruited on the Prolific platform (`https://www.prolific.co/`). This is consistent with recommended participant group sizes in Q-methodology [75]. Based on the pilot study timings, we paid participants £3 for 20 minutes of labour, exceeding the UK minimum wage. Ethical approval was obtained from our ethical review board. Participants did not provide any personal data, ensuring that participation was anonymous.

4. Analysis & Findings

We extracted factors using the centroid technique and applied a varimax procedure for factor rotation. Factors with an eigenvalue in excess of 1.00, and having at least two significantly loading participants, were selected for interpretation (as recommended in [75]). The composite Q-sort for each factor is included in Appendix A. In this section, Pi refers to a comment by Participant i.

Factor A: People are focused on themselves and driven by habit (Figure 3).

Demographic information: Factor A has nine significantly loading participants (5M/4F) with an average age of 31.78 years. It explains 14% of the study variance with an eigenvalue of 9.48.

Factor interpretation: One of the strongest opinions here is that non-compliance is due to dishonesty (14: +3). As P3 said: "*Dishonest people care less about boundaries in place, so they are more likely to do what they want and not what is best for everyone*." P22 said "*Some people are only interested in personal benefit irregardless of regulations, or if they are negatively affecting someone else*." The influence of habit (19: +3) is important, as "*... people will often automatically do whatever it is they are most used to doing and it is often either difficult or worrying to change behavior. Sometimes I think people don't even realise that they're doing something that could be improved*." (P3). Behavior is also influenced by national culture (7: +2) and the "*media and television*" (P25). It's not troublesome, too difficult, or impossible to follow the rules (16: -3; 3: -2), as P13 explains "*... it's all about self-commitment and often people just don't want to make the effort*." P20 agreed that "*I don't think there is any difficulty in following any kind of rule as long as the rule doesn't involve disclosing personal data for malicious reasons*." People are not finding alternative workarounds to cyber security requirements (15: -3). P19 stated: "*unfortunately, I think there are no convenient alternatives to cyber security, especially in modern workspaces*." People are interested in cyber security up to a point (23: -2; 26: +1), for example "*... people will get security apps on their devices and assume that they are fine from there ...*" (P3). P34 stated: "*I think with the modern technology we have and use every day, it's hard not to want to protect yourself ... [people] comply to a point where [they] think they're safe*." People may lack knowledge and awareness of cybersecurity (13: +2) and because they are overloaded with work (10: +2) people "*do not have the time to think about cyber security*" (P35).

Factor B: People don't like change and are not sufficiently informed to comply. (Figure 4). *Demographic information:* Factor B has six significantly loading participants (1M/5F) with an average age of 33 years. It explains 12% of the study variance with an eigenvalue of 3.29.

Factor interpretation: People prefer to do what they are used to doing (19: +3) and "don't like changes in their routine or in the way they always do things" (P38). As P12 states: "*humans are creatures of habits [sic].*" People will comply up to a point (26: +2) but "[generally] *resent being told what to do. They are prepared to follow rules to an extent, but if those rules begin to inconvenience them they will stop complying with them*." (P18). Instead of it being difficult to follow the rules (16: -2) it's "*more the question of not wanting to*" (P38) and people considering themselves above the rules (22: +2). As P39 explains: "*There are always people in workplaces who deem themselves above the rules and don't think rules apply to them. Not just cyber rules but all rules!*" These participants strongly disagreed with the notion that cyber security gets in the way of people doing their jobs (4: -3). P37 says "*It ensures security for the user and that's what matters most*." People don't have sufficient knowledge and awareness of cyber security (13: +3) and "*computers, the internet and how to be safe online*" (P12). People are not interested in cyber security (23: -1) and "*unless [you are] technically minded, cyber security is boring*" (P18). Considering neutralisation techniques (1: -1) there "*isn't any valid justification for not following the rules. Rules are in place for a reason*." (P18).

Factor C: People comply up to a point and then look for workarounds (Figure 5). *Demographic information:* Factor C has three significantly loading

participants (2M/1F) with an average age of 38.33 years. It explains 8% of the study variance with an eigenvalue of 2.82. *Factor interpretation:* People comply up to a point (26: +3) but "*do not want security as an extra work, or we just don't perceive it as an important problem*" (P28). P27 further elaborates that "*Sometimes cyber securities rules or restrictions are just too much. At that point you start looking for workarounds. For instance, now that I work from home mostly, I get frustrated with all the extra rules and the performance issues it causes. So, if I want to work comfortably at something I email it to my personal email address and work at it on my home pc.*" Compliance is "*something we take from our environment*" (P16) and influenced by national culture (7: +3). People also copy the behavior of colleagues (9: +2) as "*sometimes people don't really have their own opinion so they attach themselves to someone else's*" (P16). People have "*... modern technology. Everyone can see consequences of not following the rules. It's their choice not to follow them*" (P16) and lack of physical resources is not the issue (12: -2). People have sufficient knowledge and awareness (13: -3), and agree with the rationale (25: -3). P27 commented "*I think people have been bombarded with information on cybersecurity. Especially in a corporate environment. Most people know enough. But it is as with eating and exercising. You know what is good for you, but how many people choose to do the exact opposite?*" Cyber security does not align well with personal values (17: +1) and "*the user is an afterthought. That is what frustrates people. The want the rule makers to be aware of what they want and need, and them to come up with a solution that allows them to behave as they want and be safe at the same time*" (P27).

Factor D has both positive and negative significant loadings and is thus a bipolar factor. It has an overall eigenvalue of 2.73. It has been split to produce two distinct factor interpretations [75], described as D1 and D2 below.

Factor D1: People think they know better and are influenced by colleagues in justifying non-compliance (Figure 6). *Demographic information:* Factor D has four significantly loading participants (4M) with an average age of 29 years. It explains 9% of the study variance with an eigenvalue of 2.72.

Factor interpretation: Participants strongly agreed that people considered themselves too smart to follow the rules (22: +3). P8 said: "*People have huge ego's but don't know much about IT at all so they will call you asking for help and then when you tell them they will say they know better.*" behavior is influenced by national culture (7: +2) as "*it is the environment that we are brought up in that influences us the most*" (P31). People copy the behavior of their colleagues (9: +3). There is a perception that people can "*justify why the rules don't apply to them*" (P4) and thus don't follow the rules (1: +2). However, people can expect "*a good chance that we will answer for our deeds*" as P31 states (2: -3). Following the rules does not violate personal privacy (18: -2) as "*cyber security rules are used to maintain privacy*" (P26).

Factor D2: People are not interested in cyber security, but are driven by external rewards (Figure 7). *Demographic information:* Factor E has two significantly loading participants (2M) with an average age of 22.5 years. It explains 9% of the study variance with an eigenvalue of 1.92.

Factor interpretation: These participants do not agree that people will try to justify why they do not need to follow the rules (1: -3), nor do they believe that people do not face consequences for non-compliance (5: -2) or that people comply up to a point and then give up (26: -1). P32 says: "*I believe that everyone person knows or at least has the thought the karma may hit them if they don't follow the rules properly.*"

They do, on the other hand, consider that people are not interested in cyber security (23: +3), are not committed to cyber security (24: +3), and that following the rules would violate their personal privacy (18: +2). P32 said "*I know a lot of people who did cyber security and ended up dropping the coarse they lost interest and become dishonest with themselves, and realising over time they only did it for the external rewards but soon realised it wasn't what they where passionate about, then eventually dropped the course has a whole.*" Following the rules violates personal privacy (18: +2) and there is a feeling that the rules do not align with personal values (17: -3) because "*the rules are made by giant corporations and therefore do not respect personal values*" (P1).

Factor E: People comply up to a point, but lack knowledge and become frustrated (Figure 8). *Demographic information:* Factor E has six significantly loading participants (6F) with an average age of 41.33 years. It explains 7% of the study variance with an eigenvalue of 1.92.

Factor interpretation: These participants do not believe that people are affected by the behaviors of their peers (9: -3). P21 says "*How people work online is a personal thing, so I don't think someones actions would necessarily be influenced by someone else.*" People will comply up to a point, but feel frustrated with cyber security requirements (26: +3; 20: +3). They lack knowledge and awareness of cyber security (13: +2). As P23 explains, "*lack of knowledge about the topic means terminology can be confusing which for lots of*

users means they stop paying attention and ignore things which could be problems." P21 illustrates the lack of understanding by stating: "*People don't fully understand the why cyber security measures are in place and the implications if it wasn't. Until someone is personally affected by it, it's always something that happens to other people*." A further issue is that people lack physical resources to follow the rules (12: +1). On the other hand, they do believe that people lack the resources to follow the rules (12: +1). P23 says: "*Often good quality security add ons can be expensive and if people don't know what they are all about they wont pay for something if they are not sure why they need it!*" A problematic combination is a lack of knowledge and cost, as P23 explains, "*often good quality security add-ons can be expensive and if people don't know what they are all about they won't pay for something if they are not sure why they need it!*" The behavior of colleagues is not a big factor in non-compliance (9: -3) as "*how people work online is a personal thing, so I don't think someone's actions would necessarily be influenced by someone else*" (P21). Violation of personal privacy is not an issue, as "*... these measures are in place to protect it*" (P21).

5. Discussion & Conclusion

The six factors we uncovered overwhelmingly attribute non-compliance to individuals, their cognitions, knowledge, habits and frustrations. Only one mentions the fact that people are influenced by the behaviors of their peers (social capital), a powerful influence [76, 77] that should be given far more acknowledgement. Moreover, there is little mention of the other habitus capital factors which were revealed by our research literature review. Our participants did not agree that cultural or economic capital types influenced cyber security behaviors.

Our study thus reveals an *attribution gulf*. While researchers have highlighted the influence of a range of non-compliance causatives, many of which align with habitus concepts, the general public still attributes non-compliance to individual users' deliberate and flawed behaviors.

Why is this a problem? Because the situation is far more complex and non-compliance reasons do not arise purely from the minds and hearts of individual users without any reference to their context and standing within their communities. If we attribute the problem to individuals, our interventions will also focus on individuals, and non-compliance will not be reduced in any meaningful way.

It should be emphasized that this analysis reveals opinions i.e. how people see things. While the relatively small number of participants (40) would be too small to demonstrate statistical significance, it is methodologically appropriate for detecting cultural opinions [75], which is what we aimed to achieve.

We ought to design interventions to reduce non-compliance by acknowledging the habitus-related factors. So, for example, if we address the intervention towards the entire team who work and collaborate, to develop a social compliance norm, we have a much better chance of succeeding. We also have to be very careful not to reduce status in front of peers, because that is likely to have the opposite effect.

References

[1] M. Siponen, S. Pahnila, and M. A. Mahmood, "Compliance with information security policies: An empirical investigation," *Computer*, vol. 43, no. 2, pp. 64–71, 2010.

[2] P. B. Lowry and G. D. Moody, "Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies," *Information Systems Journal*, vol. 25, no. 5, pp. 433–463, 2015.

[3] K. Renaud, "Blaming noncompliance is too convenient: What really causes information breaches?," *IEEE Security & Privacy*, vol. 10, no. 3, pp. 57–63, 2011.

[4] E. H. Ferneley and P. Sobreperez, "Resist, comply or workaround? An examination of different facets of user engagement with information systems," *European Journal of Information Systems*, vol. 15, no. 4, pp. 345–356, 2006.

[5] I. Kirlappos, S. Parkin, and M. A. Sasse, "Learning from "shadow security": Why understanding non-compliance provides the basis for effective security," in *Proceedings USEC '14*, (San Diego, CA, USA), 23 February 2014.

[6] P. Mascini, "The blameworthiness of health and safety rule violations," *Law & Policy*, vol. 27, no. 3, pp. 472–490, 2005.

[7] R. Koppel, S. W. Smith, J. Blythe, and V. H. Kothari, "Workarounds to computer access in healthcare organizations: you want my password or a dead patient?," *ITCH*, vol. 15, no. 4, pp. 215–220, 2015.

[8] A. Utesheva and S. K. Boell, "Theorizing society and technology in information systems research," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 47, no. 4, pp. 106–110, 2016.

[9] J. Sterne, "Bourdieu, technique and technology," *Cultural Studies*, vol. 17, no. 3-4, pp. 367–389, 2003. DOI: 10.1080/0950238032000083863a.

[10] N. Elias and E. Jephcott, *The civilizing process*, vol. 2. Pantheon books New York, 1982.

[11] M. Karjalainen, M. Siponen, P. Puhakainen, and S. Sarker, "Universal and Culture-dependent Employee Compliance of Information Systems Security Procedures," *Journal of Global Information Technology Management*, vol. 23, pp. 5–24, Jan. 2020.

[12] G. D. Moody, M. Siponen, and S. Pahnila, "Toward a unified model of information security policy compliance," *MIS Quarterly*, vol. 42, pp. 285–312, Mar. 2018.

[13] A. Vance, M. Siponen, and S. Pahnila, "Motivating is security compliance: Insights from habit and protection motivation theory," *Information & Management*, vol. 49, no. 3, pp. 190–198, 2012.

[14] K. Renaud and J. Ophoff, "Modeling inertia causatives: validating in the password manager adoption context," in *2019 Dewald Roode Workshop on Information Systems Security Research*, p. 14, IFIP Working Group 8.11/11.13, 2019.

[15] K. Renaud, R. Otondo, and M. Warkentin, ""This is the way 'I' create my passwords" ... does the endowment effect deter people from changing the way they create their passwords?," *Computers & Security*, vol. 82, pp. 241–260, 2019.

[16] C. Perrow, *Normal accidents: Living with high risk technologies-Updated edition*. Princeton University Press, 2011.

[17] P. Bourdieu, *The logic of practice*. Stanford University Press, 1990.

[18] Z. Papacharissi and E. Easton, "In the habitus of the new," *A companion to new media dynamics*, pp. 171–184, 2013.

[19] P. Bourdieu, *Distinction: A social critique of the judgement of taste*. Harvard University Press, 1984.

[20] P. Bourdieu and J. G. Richardson, "Handbook of theory and research for the sociology of education," *The Forms of Capital*, pp. 241–258, 1986.

[21] S. Davies and J. Rizk, "The three generations of cultural capital research: A narrative review," *Review of Educational Research*, vol. 88, no. 3, pp. 331–365, 2018.

[22] A. Carlson and A. M. Isaacs, "Technological capital: An alternative to the digital divide," *Journal of Applied Communication Research*, vol. 46, no. 2, pp. 243–265, 2018.

[23] D. Calderón Gómez, "Technological capital and digital divide among young people: an intersectional approach," *Journal of Youth Studies*, vol. 22, no. 7, pp. 941–958, 2019.

[24] D. Bell, *An introduction to cybercultures*. Routledge, 2006.

[25] A. Calderaro and A. J. Craig, "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building," *Third World Quarterly*, pp. 1–22, 2020.

[26] E. M. Redmiles, S. Kross, and M. L. Mazurek, "Where is the digital divide? a survey of security, privacy, and socioeconomics," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 931–936, 2017.

[27] N. N. Schia, "The cyber frontier and digital pitfalls in the global south," *Third World Quarterly*, vol. 39, no. 5, pp. 821–837, 2018.

[28] S. M. Debb, D. R. Schaffer, and D. G. Colson, "A Reverse Digital Divide: Comparing Information Security Behaviors of Generation Y and Generation Z Adults," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 3, no. 1, pp. 42–55, 2020.

[29] S. Morgan, "Cybersecurity talent crunch to create 3.5 million unfilled jobs globally by 2021," 2019. `https://cybersecurityventures.com/jobs/`.

[30] R. A. Angraini and O. Alias, "Information security policy compliance: Systematic literature review," *Procedia Computer Science*, vol. 161, pp. 1216–1224, 2019.

[31] W. A. Cram, J. D'arcy, and J. G. Proudfoot, "Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance," *MIS Quarterly*, vol. 43, no. 2, pp. 525–554, 2019.

[32] X. Chen, L. Chen, and D. Wu, "Factors that influence employees' security policy compliance: an awareness-motivation-capability perspective," *Journal of Computer Information Systems*, vol. 58, no. 4, pp. 312–324, 2018.

[33] J. J. Jiang, W. A. Muhanna, and G. Klein, "User resistance and strategies for promoting acceptance across system types," *Information & Management*, vol. 37, no. 1, pp. 25–36, 2000.

[34] J. M. Blythe, L. Coventry, and L. Little, "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 103–122, 2015.

[35] G. Bansal, S. Muzatko, and S. I. Shin, "Information system security policy noncompliance: the role of situation-specific ethical orientation," *Information Technology & People*, 2020.

[36] S. Altamimi, K. Renaud, and T. Storer, ""I do it because they do it": social-neutralisation in information security practices of Saudi medical interns," in *International Conference on Risks and Security of Internet and Systems*, pp. 227–243, Springer, 2019.

[37] K. L. Gwebu, J. Wang, and M. Y. Hu, "Information security policy noncompliance: An integrative social influence model," *Information Systems Journal*, 2019.

[38] A. Hovav and J. D'Arcy, "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea," *Information & Management*, vol. 49, no. 2, pp. 99–110, 2012.

[39] S. Trang and B. Brendel, "A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research," *Information Systems Frontiers*, vol. 21, pp. 1265–1284, Dec. 2019.

[40] K. H. Guo and Y. Yuan, "The effects of multilevel sanctions on information security violations: A mediating model," *Information & Management*, vol. 49, no. 6, pp. 320–326, 2012.

[41] Y. J. Li and E. Hoffman, "Information security policy compliance," *SSRN Electronic Journal*, 2018.

[42] A. Song, *Evaluation of the Intents of Noncompliance with the Organizational Information Systems Security Policy*. PhD thesis, University of Phoenix, 2018.

[43] I. Hwang, D. Kim, T. Kim, and S. Kim, "Why not comply with information security? an empirical approach for the causes of non-compliance," *Online Information Review*, 2017.

[44] H. L. Kim and J. Han, "Do employees in a "good" company comply better with information security policy? A corporate social responsibility perspective," *Information Technology & People*, vol. 32, pp. 858–875, Jan. 2019.

[45] H. C. Pham, D. D. Pham, L. Brennan, and J. Richardson, "Information security and people: A conundrum for compliance," *Australasian Journal of Information Systems*, vol. 21, 2017.

[46] S. Sharma and M. Warkentin, "Do I really belong?: Impact of employment status on information security policy compliance," *Computers & Security*, vol. 87, pp. 101397–101397, 2019.

[47] K. Njenga, "Understanding internal information systems security policy violations as paradoxes," *Interdisciplinary Journal of Information, Knowledge and Management*, vol. 12, pp. 1–16, 2017.

[48] A. Silvius and T. Dols, "Factors influencing Non-Compliance behavior towards Information Security Policies," *CONF-IRM 2012 Proceedings*, May 2012.

[49] H. L. Kim, H. S. Choi, and J. Han, "Leader power and employees' information security policy compliance," *Security Journal*, vol. 32, no. 4, pp. 391–409, 2019.

[50] A. Yazdanmehr, J. Wang, and Z. Yang, "Peers matter: The moderating role of social influence on information security policy compliance," *Information Systems Journal*, vol. n/a, 2020.

[51] D. M. Ashenden, L. Coles-Kemp, and K. O'Hara, "Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen," *Politics and Governance*, vol. 6, no. 2, pp. 41–48, 2018.

[52] T. Dols and A. Silvius, "Exploring the influence of national cultures on non-compliance behavior," *Communications of the IIMA*, vol. 10, no. 3, p. 2, 2010.

[53] S. Smith, D. Winchester, D. Bunker, and R. Jamieson, "Circuits of Power: A Study of Mandated Compliance to an Information Systems Security "De Jure" Standard in a Government Organization," *MIS Quarterly*, vol. 34, no. 3, pp. 463–486, 2010.

[54] C. Lee, C. C. Lee, and S. Kim, "Understanding information security stress: Focusing on the type of information security compliance activity," *Computers & Security*, vol. 59, pp. 60–70, 2016.

[55] D. Ormond, M. Warkentin, and R. Crossler, "Integrating Cognition with an Affective Lens to Better Understand Information Security Policy Compliance," *Journal of the Association for Information Systems*, vol. 20, Dec. 2019.

[56] A. Yazdanmehr, J. Wang, and Z. Yang, "Peers matter: The moderating role of social influence on information security policy compliance," *Information Systems Journal*, pp. 1–54, 2020.

[57] T.-B. Lembcke, K. Masuch, S. Trang, S. Hengstler, P. Plics, and M. Pamuk, "Fostering Information Security Compliance: Comparing the Predictive Power of Social Learning Theory and Deterrence Theory," *AMCIS 2019 Proceedings*, July 2019.

[58] C. Torres and R. Crossler, "Information Security Compliance: A Complete Values View," *AMCIS 2019 Proceedings*, July 2019.

[59] M. Karjalainen, M. Siponen, and S. Sarker, "Toward a stage theory of the development of employees' information security behavior," *Computers & Security*, vol. 93, p. 101782, June 2020.

[60] D. C. Shelton, *Reasons for non-compliance with mandatory information assurance policies by a trained population*. PhD thesis, Capitol Technology University, 2014.

[61] J. Blythe, R. Koppel, and S. W. Smith, "Circumvention of security: Good users do bad things," *IEEE Security & Privacy*, vol. 11, no. 5, pp. 80–83, 2013.

[62] D. Sikolia and D. Biros, "Motivating Employees to Comply with Information Security Policies," *MWAIS 2016 Proceedings*, May 2016.

[63] E. Kolkowska, F. Karlsson, and K. Hedstrm, "Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method," *The Journal of Strategic Information Systems*, vol. 26, no. 1, pp. 39–57, 2017.

[64] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, and A. Vance, "What levels of moral reasoning and values explain adherence to information security rules? An empirical study," *European Journal of Information Systems*, vol. 18, pp. 126–139, Apr. 2009.

[65] O. A. Randle and M. Yolanda, "Critical factors influencing employees compliance with information security policies of an organization: Systematic review and meta-analysis," *2017 International Conference on Information Society (i-Society)*, 2017.

[66] D. Reddy and G. Dietrich, "Unlocking the Mixed Results of the Effect of Self-Efficacy in Information Security on Compliance.," *AMCIS 2019 Proceedings*, July 2019.

[67] T. Stafford, G. Deitz, and Y. Li, "The role of internal audit and user training in information security policy compliance," *Managerial Auditing Journal*, vol. 33, pp. 410–424, Jan. 2018.

[68] J. D. Wall and M. Warkentin, "Perceived argument quality's effect on threat and coping appraisals in fear appeals: An experiment and exploration of realism check heuristics," *Information & Management*, vol. 56, p. 103157, Dec. 2019.

[69] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proceedings of the 2008 New Security Paradigms Workshop*, pp. 47–58, 2008.

[70] K. Hedström, F. Karlsson, and E. Kolkowska, "Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale," *Information Management & Computer Security*, vol. 21, no. 4, pp. 266–287, 2013.

[71] B. Stanton, M. F. Theofanos, S. S. Prettyman, and S. Furman, "Security fatigue," *IT Professional*, vol. 18, no. 5, pp. 26–32, 2016.

[72] W. Stephenson, "Correlating Persons Instead of Tests," *Journal of Personality*, vol. 4, no. 1, pp. 17–24, 1935.

[73] S. C. Weller, "Cultural consensus theory: Applications and frequently asked questions," *Field methods*, vol. 19, no. 4, pp. 339–368, 2007.

[74] S. R. Brown, "A Primer on Q Methodology," *Operant Subjectivity*, vol. 16, pp. 91–138, Apr. 1993.

[75] S. Watts and P. Stenner, "Doing Q methodology: theory, method and interpretation," *Qualitative Research in Psychology*, vol. 2, no. 1, pp. 67–91, 2005.

[76] M. Granovetter, "Threshold models of collective behavior," *American Journal of Sociology*, vol. 83, no. 6, pp. 1420–1443, 1978.

[77] W. O. Bearden, R. G. Netemeyer, and J. E. Teel, "Measurement of consumer susceptibility to interpersonal influence," *Journal of Consumer Research*, vol. 15, no. 4, pp. 473–481, 1989.

Factor Statement Loadings

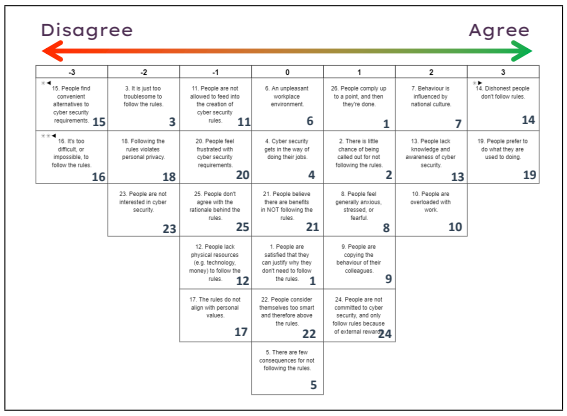

Figure 3. Factor A Q-Sort

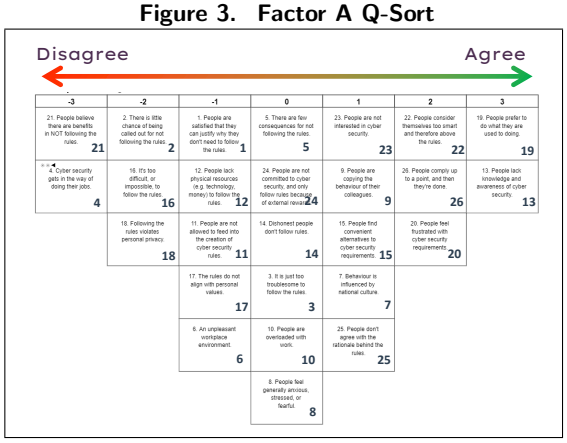

Figure 4. Factor B Q-Sort

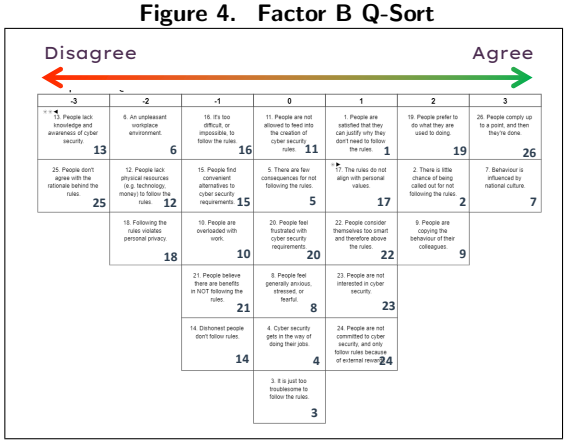

Figure 5. Factor C Q-Sort

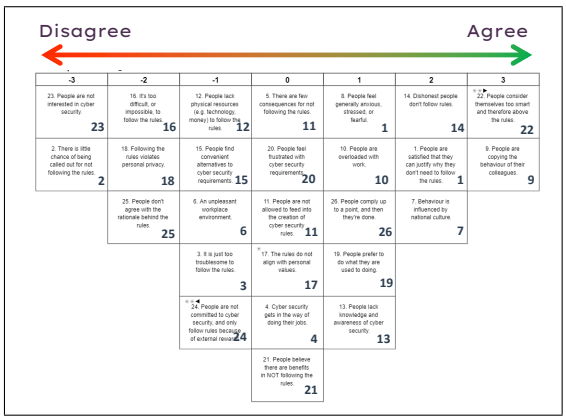

Figure 6. Factor D1 Q-Sort

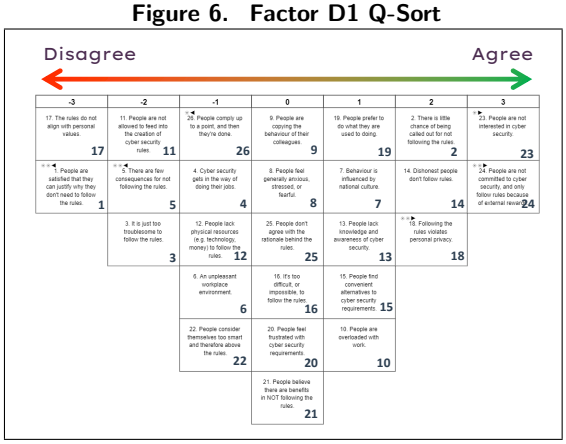

Figure 7. Factor D2 Q-Sort

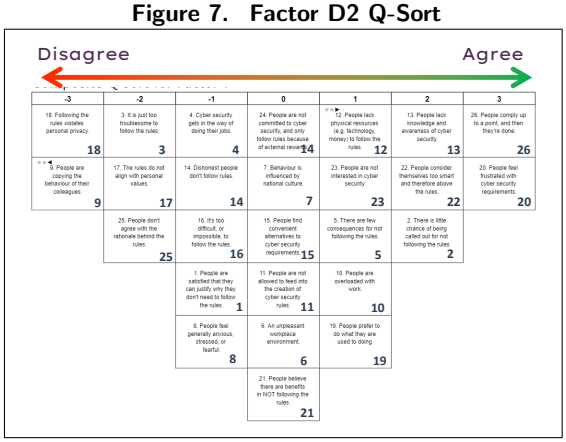

Figure 8. Factor E Q-Sort